European Cooperation
in Science and Technology
- COST -

Secretariat

Brussels, 4 July 2012

COST 4135/12

MEMORANDUM OF UNDERSTANDING

Subject : Memorandum of Understanding for the implementation of a European Concerted Research Action designated as COST Action IC1204: Trustworthy Manufacturing and Utilization of Secure Devices

Delegations will find attached the Memorandum of Understanding for COST Action as approved by the COST Committee of Senior Officials (CSO) at its 185th meeting on 6 June 2012.

MEMORANDUM OF UNDERSTANDING
For the implementation of a European Concerted Research Action designated as

COST Action IC1204
TRUSTWORTHY MANUFACTURING AND UTILIZATION OF SECURE DEVICES

The Parties to this Memorandum of Understanding, declaring their common intention to participate in the concerted Action referred to above and described in the technical Annex to the Memorandum, have reached the following understanding:

1. The Action will be carried out in accordance with the provisions of document COST 4154/11 "Rules and Procedures for Implementing COST Actions", or in any new document amending or replacing it, the contents of which the Parties are fully aware of.

2. The main objective of the Action is to identify new design and manufacturing flows for the production of secure integrated circuits by creating a strong network between several centres of expertise on hardware security at European level.

3. The economic dimension of the activities carried out under the Action has been estimated, on the basis of information available during the planning of the Action, at EUR 52 million in 2012 prices.

4. The Memorandum of Understanding will take effect on being accepted by at least five Parties.

5. The Memorandum of Understanding will remain in force for a period of 4 years, calculated from the date of the first meeting of the Management Committee, unless the duration of the Action is modified according to the provisions of Chapter V of the document referred to in Point 1 above.

———————————

A. ABSTRACT AND KEYWORDS

Hardware security is becoming increasingly important for many embedded systems applications ranging from small RFID tag to satellites orbiting the earth. Its relevance is expected to increase in the upcoming decades as secure applications such as public services, communication, control and healthcare will keep growing. The vulnerability of hardware devices that implement cryptography functions (including smart cards) has become the Achilles's heel in the last decade. Therefore, the industry is recognizing the significance of hardware security to combat semiconductor device counterfeiting, theft of service and tampering.

This COST Action aims at creating a European network of competence and experts on all aspects of hardware security including design, manufacturing, testing, reliability, validation and utilization. The network will play a key role in developing solutions responding to the hardware security challenges, hence strengthening the position of Europe in the field.

Keywords: Trustfulness of Secure Device Manufacturing, Test and Security of Secure ICs, Fault Attacks, Hardware Trojans, Reconfigurable Devices for Security

B. BACKGROUND

B.1 General background

Security is a critical part of information and communication technologies and it is the necessary basis for obtaining confidentiality, authentication, and integrity of data. The importance of security is confirmed by the extremely high growth of the smart-card market in the last 20 years. It is reported in "Le monde Informatique" in the article "Computer Crime and Security Survey" in 2007 that financial losses due to attacks on "secure objects" in the digital world are greater than $11 Billions. Since the race among developers of these secure devices and attackers accelerates, also due to the heterogeneity of new systems and their number, the improvement of the resistance of such components becomes today's major challenge.

Concerning all the possible security threats, the vulnerability of electronic devices that implement cryptography functions (including smart cards, electronic passports) has become the Achilles's heel in the last decade. Indeed, even though recent crypto-algorithms have been proven resistant to cryptanalysis, certain fraudulent manipulations on the hardware implementing such algorithms can allow extracting confidential information. So-called *Side-Channel Attacks* have been the first type of attacks that target the physical device. They are based on information gathered from the physical implementation of a cryptosystem. For instance, by correlating the power consumed and the data manipulated by the device, it is possible to discover the secret encryption key. Nevertheless, this point is widely addressed and integrated circuit (IC) manufacturers have already developed different kinds of countermeasures.

More recently, new threats have menaced secure devices and the security of the manufacturing process. A first issue is the trustworthiness of the manufacturing process. From one side, secure devices must assure a very high production quality in order not to leak confidential information due to a malfunctioning of the device. Therefore, possible defects due to manufacturing imperfections must be detected. This requires high-quality test procedures that rely on the use of test features that increases the controllability and the observability of inner points of the circuit. Unfortunately, this is harmful from a security point of view, and therefore the access to these test features must be protected from unauthorized users. Another harm is related to the possibility for an untrusted manufacturer to do malicious alterations to the design (for instance to bypass or to disable the security fence of the system). Nowadays, many steps of the production cycle of a circuit are outsourced. For economic reasons, the manufacturing process is often carried out by foundries located in foreign countries. The threat brought by so-called *Hardware Trojans*, which was long considered theoretical, begins to materialize. Advanced techniques are necessary to prevent and detect such Hardware Trojans. The US Department of Defense (DoD) responded to this growing threat by launching, in 2006, the DARPA *Trust in IC* program, a new research project that aims to find consistently reliable methodology for discovering compromised circuitry.

A second issue is the hazard of faults that can appear during the circuit's lifetime and that may affect the circuit behaviour by way of soft errors or deliberate manipulations, called *Fault Attacks*. They can be based on the intentional modification of the circuit's environment (e.g., applying extreme temperature, exposing the IC to radiation, X-rays, ultra-violet or visible light, or tampering with clock frequency) in such a way that the function implemented by the device generates an erroneous result. The attacker can discover secret information by comparing the erroneous result with the correct one. In-the-field detection of any failing behaviour is therefore of prime interest for taking further action, such as discontinuing operation or triggering an alarm. In addition, today's smart cards use 90nm technology and according to the various suppliers of chip, 65nm technology will be effective on the horizon 2013-2014. Since the energy required to force a transistor to switch is reduced for these new technologies, next-generation secure systems will become even more sensitive to various classes of fault attacks.

B.2 Current state of knowledge

The common industrial practice recognizes the threats emanating from the test of secure devices. Currently, security is achieved by physically disconnecting the access to test features after production testing, for instance, by blowing anti-fuses located at both ends of the test access mechanism. However, this solution makes the test of the device during its life cycle impossible. So far, no commercial test flows or appropriate test protocol standard are available to tackle the test/security requirements antagonism. One innovation targeted by this Action is to define new techniques that will allow full testability guaranteeing high security at the same time, at any time of the life cycle of the device.

On the other hand, Hardware Trojan detection still remains a big unresolved issue. No truly efficient techniques have been published till now. The Action will allow a strong exchange and brainstorming among all partners and therefore to substantially increase the possibility to find new solutions for this cross-disciplinary issue.

Concerning fault attacks, several papers have been published on attacks and countermeasures.

However, no accurate electrical models of fault injections exist yet. Even if it is possible to find fault models for older technologies, the compact modelling of effects of key fault injection techniques such as laser irradiation on 65nm (and beyond) circuit technology still remains an open issue. Moreover, the integration of countermeasures in computer-aided design (CAD) tools is not mature yet. The Action will cover all these missing aspects.

A COST Action would be therefore of great benefit to create a strong network among the current European research and industrial groups already focused on different aspects of hardware security, to allow idea-sharing and to define the new production flows that will guarantee higher security.

B.3 Reasons for the Action

As anticipated by Eurosmart (the association of Smart Security Industry), the volume growth of secure devices was equal to 11% in 2010 (compared to 2009) and it is expected to be more than 13% in 2011. This trend will definitely accelerate thanks to the development of several applications. Besides traditional markets (i.e., telecommunications, payment, identification and health, pay-TV, transport), the expansion of Machine To Machine (M2M) architectures is particularly promising because it opens the way for the so-called Internet of Objects.

Europe has a strong interest in being among the world's leaders in the design of trustworthy secure devices, therefore it is a critical time to gather a network of expertise on a field that could decide the future of European electronic manufacturing and design industry in a competitive globalized economy. In August 2011, VISA (the payment technology's leader) announced new policies that will give U.S. banks a reason to issue smart cards starting in 2015 (while, at the present time, they still rely on black-magnetic-stripe credit cards). This will increase even more the competition against non-European companies.

The COST Action will represent the basis of a productive and long-term collaboration between researchers with expertise in design, manufacturing, testing, and validation of secure devices. The overall outcome of the Action will be the identification of new design and manufacturing flows for the production of secure integrated circuits by creating a strong network between several centres of expertise on hardware security at European level.

B.4 Complementarity with other research programmes

Security, reliability, dependability and testability of electronic circuits are scientific topics of high importance, which is reflected by a number of European and national research projects. However, the connection between these fields is unique to this COST Action. Below, relevant recent European programmes are listed and the differences to this COST Action are briefly highlighted.

FP7 PRESERVE (2011–2014, http://www.preserve-project.eu/): Hardware Security Module (HSM) ASIC for Vehicle-2-X communication. One main objective is development, verification and prototype implementation of a sufficiently fast HSM for secure key-storage and acceleration of ECC crypto operations. The experiences from this process are relevant in the scope of this COST Action while at the same time PRESERVE would benefit from the network of expertise available through this COST Action.

FP7 EVITA (2008–2011, http://evita-project.org): E-safety vehicle intrusion protected applications. This project focused on secure devices in one particular application domain (automotive). Its main objective is development, verification and prototype implementation of a secure on-board network. The results on tampering protection are relevant in the scope of this COST Action.

FP7 MOGENTES (2008–2011, https://www.mogentes.eu/): Model-based Generation of Tests for Dependable Embedded Systems. The cross-domain modelling approaches and test and verification of the resulting models were the topics of the project. Security aspects were not considered. Work on fault injection can benefit this COST Action.

COST INTELLISYS (started 2009, http://www.intellicis.eu/): Intelligent Monitoring, Control and Security of Critical Infrastructure Systems. INTELLISYS focuses on security of critical infrastructure, emphasizing aspects such as decentralization and agent collaboration. Although security threats can originate from hardware devices, INTELLISYS does not consider hardware aspects explicitly.

FET UNIQUE (started 2009, http://www.unique-project.eu/): Foundations for Forgery-Resistant Security Hardware. This project focuses on methods to prevent counterfeiting of hardware blocks. Some aspects of the project are relevant for this Action. This includes Physically Unclonable Functions (PUF) which have been developed and manufactured within the UNIQUE project. However, no test-related security threats are considered.

FP7 DIAMOND (started 2010, http://www.fp7-diamond.eu/): Diagnosis, Error Modelling and Correction for Reliable Systems Design. This project deals with test, diagnosis and debug methods. It does not cover security violations.

CATRENE eGo (started 2010): Within this project, novel secure near-field communication approaches are developed. The possibility of security attacks is taken into account but no active investigations are performed or countermeasures developed.

CATRENE TOETS (started 2009): Towards one European Test Solution. This project develops a number of test technologies with a special focus on analog and mixed-signal circuits. Security aspects are targeted only for the definition of secure test protocols.

C. OBJECTIVES AND BENEFITS

C.1 Aim

The aim of the Action is to identify new design and manufacturing flows for the production of secure integrated circuits by creating a strong network between several centres of expertise on hardware security at European level, and to substantially increase the level of cooperation and consequent visibility of European research on this vital topic.

C.2 Objectives

The main objectives of this Action are (i) the knowledge creation to respond to new issues, and (ii) the consolidation of the scientific excellence in the target domain through the integration of the research skills of the participants.

From a scientific perspective, this project targets the following goals:

- To provide solutions for required but conflicting relationships between Testability and Security. The expected impact is a new generation of more secure and more testable products in a field where European IC industry has a leadership position to maintain
- To develop innovative design-for-testability Computer-Aided Design (CAD) tools for supporting security issues and with a specific attention to compliance with existing commercial tools
- To define secure protocols to protect the access to necessary test infrastructures and to design secure access controllers
- To contribute in the definition of new test standards that intrinsically include security issues
- To study new mechanisms for devices identification and authentication based on the usage of Physically Unclonable Functions (PUFs) and True Random Number Generators (TRNGs)
- To address issues related to counterfeiting and Hardware Trojan insertion and to propose new methods and algorithms for their identification
- To define new architectures able to detect faults and to resist to fault attacks
- To establish a design and synthesis flow, which will transform a given circuit into a secure design incorporating counter-measures against fault attacks
- To explore implementation and security issues of cryptographic logic based on Field-Programmable Gate Array (FPGA)
- To collect statistically significant data related to fault injection campaigns
- To explore formal verification methods to establish the robustness of a secure device against fault attacks

From the networking point of view, this Action is anticipated to aid towards the development of early-stage faculty researchers into experts in their respective fields, and improve the knowledge and skills of Ph. D. students and post-doctoral fellows, which will enable them to perform high-quality research. Moreover, it will support mobility between participating research centres, both of senior researchers to foster exchange of ideas through short term visits, and of junior researchers/PhD students to enable the exchange of technical knowledge through longer term visits.

Dissemination activities will be carried out by joint papers in international journals and conference proceedings, and through the organization of special sessions at international conferences.

C.3 How networking within the Action will yield the objectives?

The targeted scientific objectives of this Action will be realised through close and strong collaboration between the Action members (industry, research centres and academia). Three main strategies will be used to facilitate the realisation of the Action objectives.

- *Exchange of researchers among Action members:* Short as well as long term exchange of PhD students and researchers between universities, research centres and industry is another efficient mean that will be used for the realisation of the Action objectives. This will enable knowledge transfer, improvement of the skills of PhD students and post-doc fellows, and therefore contribute to the evolution of the early-stage researchers into experts with diverse expertise in the area of hardware security. Moreover, in these scientific missions new valuable knowledge will be gathered with respect to the theory and the applications of the investigated methods and tools, as well as the foundations for future collaborations will be set.
- *Collaboration with industry*: Action members will also target starting projects with industry partners (within or outside the Action). Such collaboration helps research from academia and research centres to get more insight in the real problems related to the practicality and help them also tune their research and solutions to suit the industry demands. Having a strong collaboration with the industry is therefore the driver behind producing solutions with huge added commercial value.
- *Collaborative projects on topic related to the Action within national and European programs*: depending on the targeted objective, Action members will form consortia and propose collaborative transnational projects; this can be submitted at national or European level.

All the above will strongly contribute to the creation of a high-quality and world-class researchers and contribute to the establishment of research excellence in Europe in the Action's areas of interest. The exchange of the latest scientific results both from academia, industry and research organizations will be instrumental in achieving the Action objectives.

Also the dissemination strategies (see Section H) will not only promote the Action activities and findings, but will also attract more universities, research institutes and industry to join the Action and/or collaborate with the Action members.

C.4 Potential impact of the Action

The Action has both scientific and networking benefits. It supports cutting edge basic research in the fields of hardware secure devices through collaborative work. Thanks to the participation of industrial partners, the Action will be the mean to provide cutting-edge knowledge related to current practices to all partners and to promote the technology transfer from academy to industry. Moreover, the involvement of young scientists will be the basis for creating a scientific community that in the future will be active in this important domain.

The main scientific benefits of the Action are summarized as follows:

- To be able to design and build secure devices that are more secure and reliable than nowadays circuits. These devices play already an important role in our life, and it is expected that they will be more and more important in the next future, especially for applications such as: transportation, health, energy production, telecommunications, banking applications, leisure.
- To provide new CAD tools for supporting security issues at any level of the design and manufacturing flows
- To develop a fault simulation and evaluation environment that will be available to all partners

C.5 Target groups/end users

The field of secure hardware has historically been characterized by lack of transparency. Many problems and solutions discovered by industrial or governmental organizations have not been made public and therefore have not been accessible for the academic community. On the other hand, solutions found in academia have not received sufficient attention by the end users.

This is particularly true for Small and Medium Enterprises (SMEs) that do not have sufficient resources to closely follow the progress of the scientific community. By combining industry (including SMEs), academic institutions and research labs this COST Action serves to the following end-users:

- The research community will be exposed to specific research needs of the involved companies. The European and the global secure hardware scientific communities are substantial and are actively communicating with neighbouring disciplines such as testing, manufacturing, dependability, and embedded systems. It can be expected that some of the basic research performed in scope of this Action can be generalized to these fields.
- The industry will benefit from the interactions with the researchers and from the solutions developed. Moreover, engineers in the industry will gain exposure to state of the art in protection technologies, which they can apply for product development. This transparency is particularly beneficial for SMEs. The industry will also benefit from standardization work to be carried out within the Action. New standards will improve inter-operability of secure components without compromising trustworthiness, thus enabling or simplifying creation and distribution of security-related intellectual-property blocks.

D. SCIENTIFIC PROGRAMME

D.1 Scientific focus

Secure devices are employed in different application areas, and they can be implemented using different technologies such as application-specific integrated circuits or reconfigurable logic. This COST Action will evaluate the vulnerability of such devices to various security threats during their manufacturing and lifetime. Moreover, known countermeasures against such threats will be optimized and new defenses will be developed. Generic approaches universally applicable to various implementation technologies as well as specific methods which leverage specific properties of a given technology are in the Action’s scope. Trustworthiness is one key characteristic of a secure device, yet there are further properties that must be maintained: manufacturability, testability, high performance, low power consumption, and moderate cost. Many known countermeasures incur penalties with respect to some of these parameters.

This Action aims at a practical design and manufacturing flow that keeps the balance between the level of protection against threats and the above-mentioned characteristics.

The five scientific areas targeted by this Action cover aspects of trustworthiness and security during manufacturing and test (areas 1 and 2) and during the device's lifetime (areas 3 and 4), while area 5 focuses on validation. The members are encouraged to participate in several areas, thus promoting cross-fertilization between the areas.

Area 1: Manufacturing test of secure devices
Area 2: Trustworthy manufacturing of secure devices
Area 3: Fault attack detection and protection
Area 4: Reconfigurable devices for secure functions
Area 5: Validation, Evaluation, and Fault Injection

The first area focuses on the dichotomy between testability and security. To facilitate high-quality manufacturing test, special on-chip hardware provides access to the device‘s internal structures. This hardware constitutes vulnerability as it can be used by a malicious attacker to read out secret information from the chip or to overwrite protected data.

Within the second area, methods for Integrated Circuit (IC) authentication and Hardware Trojan (HTs) detection are studied and developed. These two topics received particular attention in the last decade due to concerns about protection of deployed ICs. IC security risks rose with the overseas fabrication facilities and the need for outsourcing the chip manufacturing processes to reduce cost. IC authentication is used for preventing IC hacking and cloning. Techniques for IC authentication leverage manufacturing variability for extracting unique signatures from every IC. Physical Unclonable Functions are example of functions that allows extracting unique signatures from every IC based on its characteristics (e.g. delay). Beyond the evident profit loss due to presence of clones on the market, clones deployment presents a risk for customers too. At the evidence, it is difficult to rely on systems embedding clones that may present poor quality compared to original and fully tested ICs. Another risk due to the fabrication outsourcing is the insertion of HTs in the ICs during manufacturing. A Trojan is used to gain access to the device's internal data or to compromise the device operation. Both IC authentication and Trojan detection techniques require significant research work to achieve high level of IC protection.

The third area considers countermeasures to detect attempted attacks during the device's lifetime. To keep the costs in terms of power consumption, area and performance in check, a cross-level approach which employs an optimal mix of techniques on different levels of abstraction is required. Generic integrated circuits and reconfigurable field-programmable gate arrays (FPGAs) are targeted.

In the fourth area, reconfiguration as a technique to make the overall system secure and trustworthy is investigated. Fault recovery and self-repair of secure devices are studied.

The fifth area provides an evaluation framework which can be applied to solutions found in areas 1 through 4 as well as to other solutions. The framework combines the capability to handle large devices by employing FPGA-based acceleration techniques with accurate models of disturbances used by attackers to induce faults in the secure devices (e.g., laser pulses).

The areas were selected in a manner that will allow member participation in more than one area, promoting in this manner the aforementioned cross-interaction between different research fields. The inclusion of new Action members at later stages is facilitated as each of the areas is broad and can expand to additional sub-topics.

D.2 Scientific work plan methods and means

The overall research activity will be split in 5 Working Groups (WGs) focus on five areas. Two WGs will concentrate on the trustworthiness of the manufacturing process, while the other three will cover all the aspects of the reliability of secure devices while they are actually used for target applications. The five WGs are:

WG 1: Manufacturing test of secure devices

1) Tools and methodologies to improve test production coverage for secure functions

Classical techniques for digital circuit testing cannot be easily used for testing of secure devices. They are based on Design-for-testability techniques that add hardware components to the circuit, aiming to provide full controllability and observability of the internal states. Because crypto-processors and other cores in a secure system must pass through high-quality test procedures to ensure that data are correctly processed, testing of crypto chips faces a dilemma. Design-for-testability schemes require high controllability and observability of the device while security necessitates minimal controllability and observability in order to better hide the secret information. Developing innovative design-for-testability techniques and test methods becomes therefore a fundamental task for manufacturing high quality secure devices.

2) Secure protocols and controllers to protect the access to necessary test infrastructures

Typical test access points are inputs and outputs of scan chains, JTAG (Joint Test Action Group) port and other mechanisms. Reinforcing the protection based on the differentiation of the test mode from the user mode is the proposed approach in the academic world. Its integration in real secure devices is still an issue. Therefore, new secure test protocols based on the use of enhanced test controllers must be investigated. Moreover, access strategies might change during the lifetime of the device and this must be taken into account.

3) Extending security for IEEE system-level test standards

Test standards like IEEE 1149 and IEEE 1500 do not explicitly take into account security issues. One important aspect of this Action is the opportunity of joining the knowledge of academic and industrial researchers to integrate security in current standards.

WG 2: Trustworthy manufacturing of secure devices

1) PUFs for precise identification of secure devices

Physically Unclonable Functions (PUFs) are hardware components with the properties of inherent uniqueness, unclonability and tamper evidence which enable a number of interesting applications. A physical token embedding a PUF can use the PUF's responses as a unique identifier. Since the response behaviour is in practice physically unclonable, even for the manufacturer of the tokens, they are effectively unforgeable. This makes PUFs a very useful tool for precise identification of secure devices, for creating custom and powerful authentication mechanisms, and for anti-counterfeiting technologies. This activity of the COST Action will focus on the study and the implementation costs of the wide variety of known PUFs, and possibly to invent new architectures.

2) Hardware Trojan detection

In order to reduce manufacturing costs, the fabrication of integrated circuits is nowadays migrating offshore, making circuits vulnerable to security compromise, functional changes, information leaks or even catastrophic system failures under specific conditions. The threat brought by Hardware Trojans, which was under-estimated for long time, begins to materialize. On the other hand, Hardware Trojans can even be an effective vehicle for destabilization of states (for terrorist or criminal organizations) and businesses (by mafias or fraudulent competitors). For this reason, Hardware Trojan detection mechanisms are becoming more important in ensuring a trustworthy hardware environment.

WG 3: Fault attack detection and protection

1) Using redundancy to detect fault attacks

Redundancy methods have been proposed to detect errors in data processed by a device embedding secret information. Error detection exploits different forms of redundancy, namely temporal (i.e., calculating twice the same function and comparing the two results), hardware (where two devices are instanced for the same function) and information redundancies (that consists in checking for possible mismatches between a code predicted for an output from the current input, and the code of the actual output of the process). The Action will investigate design methods and synthesis flow to transform an unprotected circuit into a robust design protected by such techniques.

2) Cross-level optimizations on residual weak spots in the circuit

This activity will provide a methodology for designing cost-efficient robust circuits that have limited energy budget and constraints on area overhead at the same time. The robustness will be achieved by an efficient cross-level combination of redundancy techniques. Parts of the circuit will be protected by low-level hardening techniques such as transistor upsizing or gate duplication (hardware redundancy), while the residual circuitry is protected by advanced error- detecting codes (information redundancy). Related selective hardening strategies have been applied in the past to protect circuits against random errors at low cost. Their application to security threats and the combination with information redundancy is a novel approach.

WG 4: Reconfigurable devices for secure functions

1) Mitigation architectures on FPGAs to counteract fault attacks

Many techniques have recently been developed to protect critical systems on SRAM-based FPGAs against Single Event Upset. At the design level of the FPGA these techniques are classified as mitigation techniques, which prevent faults to affect the target design, and recovery techniques that repair erroneous bits of the FPGA configuration memory. These techniques will be investigated and re-adapted to cope with the issue of fault attacks.

2) Self-repairable architectures of secure devices

New characteristics of recent commercial FPGA devices allow the partial re-configuration of the circuit implemented in it. By exploiting this inherent property of FPGAs, new implementations of self-repairable cryptographic logic based on FPGA-implemented detection and recovery mechanisms will allow correcting errors provoked by fault attacks.

WG 5: Validation, Evaluation, and Fault Injection

1) Fault-injection campaigns

The effect of laser shots into circuits will be evaluated to obtain statistically significant data on the consequences of the attacks. For that, experiments will be performed on commercial available circuits (for instance FPGAs), and circuits already available in the partners' labs. Precise models of the laser shots onto the circuit will be modelled from the conducted experiments.

2) Fault simulators for realistic fault-models

To simulate faults at different levels of abstraction (transistor, gate, register-transfer, system level), there are several methods for efficient fault simulation, including compiled, event-driven, emulated, parallel and deductive techniques. Although a variety of commercial tools are available for this purpose, they do not provide access to detailed information required in security context. One goal of this Action will be to assist in developing, by multiple involved group members, an open-source simulator able to perform both logic and fault simulation for realistic fault models extracted from the fault-injection campaigns described above. The fault injector will be enhanced by an FPGA-based emulation platform.

3) Validation

Formal verification methods that mathematically prove immunity to certain classes of malicious faults will be investigated, by using for instance techniques based on Boolean Satisfiability and Quantified Boolean Formula solvers. Accurate modelling of malicious faults is important because advanced redundancy mechanisms are developed by the information theory community and evaluated using high-level metrics, which do not capture circuit aspects. The extensive work on fault modelling that has been performed by the test community will be used to assess whether the properties of the redundant codes reported by the information theory community can be confirmed in application.

4) Evaluation

Cryptographic Engineering takes up all aspects for implementation of cryptographic algorithms in hardware (and/or software). This ranges from implementations with high performance demands implementations with hardware resource restrictions and ultra-low power implementations of cryptographic primitives, fault tolerant implementations, attack resistant implementation and implementations of attacks. This task focuses on the hardware evaluation of the cryptographic and safety solutions. Hardware measurements will be given in terms of performances, power dissipation, and amount of used hardware resources.

E. ORGANISATION

E.1 Coordination and organisation

The COST Action will be coordinated by a Management Committee (MC). The Chair and the Vice-Chair of the MC will be elected at the Kick-Off (KO) meeting to be held at the start of the Action. Each country will have two representatives in the MC. In addition, Chairs and Vice-Chairs for each Working Group, and a Web Site Coordinator will be appointed during the KO meeting.

After the KO meeting, MC meetings will take place twice a year. These meetings will deal with all strategic issues concerning the Action such as the approval of any new Working Groups, the termination of existing Working Groups, organization of the workshop, approval of Short Term Scientific Missions (STSMs), identification of the Summer School Chair/Vice-Chair, ways to improve communication between consortium partners, ways to improve dissemination of the results of the Action, or any other activity that requires the MC to be consulted. The MC will also be in charge of coordinating the editorial production of the Annual Reports of each WG, which are due at the end of each year that the Action is running. Moreover, the MC will promote Short Term Scientific Missions (STSMs) for exchange of students, as well as senior scientists, between the participating research groups. Young researchers and women scientists in particular will be encouraged to participate in such exchanges.

Annual Reports will be delivered from each WG. The first Annual Report will contain an extensive state-of-art review, the next two Annual Reports will contain the progress of the Action, and the last Annual Report will contain the conclusions of the Action. All of the WG Annual reports will be grouped in an overall Report prepared by the MC, which will describe also the main achievements of the Action. In particular, the MC Report will give a general overview of the Action development, describing the results following the objectives described in section C.2 (number of STSM, number of Workshop/Ph.D. School participants), and giving the status of the involvement of new partners in the COST Action.

One workshop will be organized at the 3rd year of the Action. The workshop will be open to the entire scientific community and can potentially be held jointly with some other conferences. The goal of the workshop would be to summarize the current status and future trends of the research field of the Action. Participants and invited speakers from European and non-European countries, will update the members of the COST Action on the most recent results.

Two summer schools for PhD students will be organized at the 2nd and the last year of the Action. The summer school will be an opportunity for young students to exchange ideas, discuss their research interests, learn the latest advances from European and non-European experts in various fields related to the manufacturability issues of secure devices.

Moreover, summer schools are a good opportunity for young people to interact with other research groups and possibly set up STSMs. The Summer School Chair will give particular attention in fostering these interactions and to encourage the subsequent students' exchange.

An extensive use of web technologies is foreseen. Under the responsibility of the Web Site Coordinator, e-mail of participants and other interested people will be collected, and a mailing list will be created. A short newsletter will be sent three/four times per year to the mailing list announcing workshops, achievements of the COST Action, summer school, call for application to the STSM, etc. A website for the Action will also be set up at the start of the Action. This website will assist in the exploitation and dissemination of the results of the Action, both externally and internally. The website will contain technical reports, source code repository, interesting deadlines for conferences, meetings, project proposals, etc. A subset of hot topics will be selected and collaborative wiki pages will be set up to provide a virtual place to discuss and provide feed-back on the most attention-grabbing research issues related to the COST Action. The WG chairs will be responsible for maintaining the website in cooperation with the Web-Chair.

E.2 Working Groups

Based on these research areas, this Action will establish 5 Working Groups (WGs) that will be responsible to complete all the scientific goals set by this Action. The objectives of these WGs were described in section D.2. WG Chairs and Vice-Chairs (who will be elected by the MC during the Kick-Off meeting) will coordinate the activities of the Working Groups, lead the scientific discussions, and provide the MC with the annual report on the progress of the Working Group.

All researchers participating in this Action will be invited to join one or more Working Groups, depending on their research interests and activities. In the course of the Action, new Working Groups can also be established depending on the needs of the Action.

The contents of the 5 Working Groups are listed in Section D.2.

E.3 Liaison and interaction with other research programmes

The projects FP7 UNIQUE and CATRENE TOETS target respectively the issue of PUFs and the test of secure devices. Interactions between these projects and this Action will be organized by exchange of information and possibly by inviting partners of the project to workshops and WG meetings organized by the Action.

E.4 Gender balance and involvement of early-stage researchers

This COST Action will respect an appropriate gender balance in all its activities and the Management Committee will place this as a standard item on all its MC agendas. The Action will also be committed to considerably involve early stage researchers. This item will also be placed as standard item on all MC agendas. To promote gender diversity and balance of the researchers involved in this Action, the Management Committee will be responsible for building and maintaining diversity in all management structures by nationality and race. Furthermore, every effort will be made to maintain a good gender balance in the elected leaders of this Action (Chair, Vice-Chair, MC members, WG leaders) who cover coordinational, organizational and other related responsibilities. In addition, early stage researchers are also invited to participate in MC meetings.

F. TIMETABLE

The Action will have a total duration of four years. Two Management Committee (MC) meetings and Working Group (WG) meetings will be held every year. Moreover, two Training Schools and one Workshop will be organized during the Action. The following table summarizes the timetable in details. A final conference will be held at the end of the Action.

Months	Year 1	Year 2	Year 3	Year 4	Year 5
1-4	- Kick-Off Meeting - Website set-up	- MC/WG Meetings	- MC/WG Meetings	- MC/WG Meetings	- Final conference
5-8		- Training School	- Workshop	- Training School	
9-12	- MC/WG Meetings - WG Report	- MC/WG Meetings - WG Report	- MC/WG Meetings - WG Report	- MC/WG Meetings - WG Report	

The Action will start with the Kick-Off (KO) Meeting, during which the Management Committee (MC) chairs/vice-chairs and Working Group (WG) leaders will be elected. After that, the Action website will be set-up.

Every MC meeting will be organized in conjunction with a WG meeting in order to reduce expenses within the Action budget. Each MC/WG event will last 2 days. The first day will be devoted to management issues and the second to the technical meetings organized by the Working Groups. At the end of every year, WGs will provide reports of their activity to be disseminated on the website. Each MC/WG meeting will take place in a different participating Member State in order to allocate organization responsibilities among each partner and promote collaboration.

One workshop and two training schools will be organized on a basis of three-day events.

Additional technical meetings can be organized ad-hoc outside the MC meetings if necessary.

Finally, it is expected that after the Kick-Off meeting and for the duration of the Action, there will be several Short Term Scientific Missions (STSM) among the different research groups.

G. ECONOMIC DIMENSION

The following COST countries have actively participated in the preparation of the Action or otherwise indicated their interest: BE, CH, CZ, DE, EL, FR, IT, NL, PT, SE, SI, SK, UK. On the basis of national estimates, the economic dimension of the activities to be carried out under the Action has been estimated at 52 Million € for the total duration of the Action. This estimate is valid under the assumption that all the countries mentioned above but no other countries will participate in the Action. Any departure from this will change the total cost accordingly.

H. DISSEMINATION PLAN

H.1 Who?

The overall objective of the dissemination activity is to ensure that knowledge, the findings, experience and recommendations gained during this Action are shared as widely as possible and reused, both internally (with the COST Action members) and externally (outside the members border).

Internal targeted audience consists of all COST Action members, both from Academia and industry. These are the European main players in the field of design, manufacturing and utilization of secure devices.

External targeted audience consists of all people and institutions/companies working in the field as well as international bodies and organisation which are somehow related to the field. Examples of external targeted audience are:

- International research community in the field of hardware security, including design, manufacturing, test, packaging, and utilization/application.
- Other related research frameworks (such as FP7) and other COST Actions; e.g., consortia involved in European projects in the field of hardware security.

- Regional and international industry involved in the field of hardware security including semiconductor companies (fab-less, fab-lie and Integrated Device Manufacturer (IDM)), IC developers, system developer, system integrators, Original Equipment Manufacturer (OEM) and system users, etc.
- Professional bodies such as the IEEE and standardisation groups.
- Trade and professional magazines to make the findings accessible for both professional around the world as well as the general public.

H.2 What?

Dissemination will be carried out at regional, national and international level as appropriate. A mix of dedicated channels will be used in order to reach the target groups of decision makers and citizens and to inform them about our findings of the Action. Four strategies will be used for the dissemination of obtained results as described next.

1) Presentation through renowned conferences and journals

All Action partners are encouraged to present their work in leading national and international conferences and journals and contribute to information dissemination events such as organising special sessions and providing tutorials at leading conferences, briefing days, exhibitions, poster sessions, etc. This will support on one hand to demonstrate the technical achievements and on the other hand to make the technology better known outside the consortium and facilitate the prospects for future commercialization for applications under development.

2) Communication through Action members and their contacts and networks

All Action members will use their established business contacts, networks, Working Groups and user groups and workshops to inform internal and external members about the Action findings and results. All of these activities will increase the impact, visibility and dissemination of Action results.

3) Project website

In cooperation with all members, a website will be created. Access to this site will be promoted to as much people as possible through other dissemination activities. All members will contribute to information updating and communications and the Action coordinator will ensure a quality control on the website administration. A private area will provide a means of inter-action communication. The website will be linked and accessible from all members websites.

4) Training and education

Industrial training and academic education activities are targeted to creating the skilled personnel of the future through a synergy between academic and industrial groups that will foster the generation of new ideas, discoveries and processes as well as the exploitation of the related results.

H.3 How?

This COST Action meets not only the needs of research communities in Europe, but also the requirements semiconductor companies (fab-less, fab-lite, IDM), IP developers, system developers, system integrators and OEMs with emphasis on trustworthy and secure hardware needs. The dissemination and exploitation of the results developed in the course of the Action targets the findings of the Action at different aspects of the activities involved, including design, manufacturing, test, fault attack detection & protection, reconfigurable devices for secure applications, etc. Such a dissemination/exploitation plan takes into consideration finding appropriate channels and paths to targeted market depending on the results to be exploited. For instance, test technology community and IDM will be more interested in results related to design-for-testability and test solutions for secure devices

It is worth noting that the Action will participate in platforms and coordinating actions, and will focus on industry-academia collaboration by allowing Industry members to take on a consulting role especially towards young researchers and shape the research effort.

It is also worth mentioning that the efforts will focus towards the enlargement of the Action’s size by attracting and including additional important partners from the European research community in the field of hardware security and related topics and their applications. The website will host invitations to join the Action and recruitment of new partners and open research positions related to the Action’s activities will be announced.